

CLAIMS

1 1. A method for defining sets of encryption keys from a key matrix, comprising:
2 receiving at least one parameter representing a characteristic of the key matrix;
3 using the parameter and an error-correcting code, defining plural sets of keys; and
4 assigning at least some sets of keys to at least some respective devices.

1 2. The method of Claim 1, wherein the error-correcting code is a Reed-Solomon code.

1 3. The method of Claim 1, wherein each set of keys represents a set of key indices in
2 the key matrix, each key index being associated with a respective key.

1 4. The method of Claim 1, wherein the receiving act includes receiving at least a row
2 parameter "N" representing the number of rows in the key matrix and a column parameter "n"
3 representing the number of columns in the key matrix, and the method further includes:
4 using an error-correcting code having a Hamming distance "d" that minimizes key
5 overlap between sets of keys.

1 5. The method of Claim 4, wherein the error-correcting code defines the sets of keys
2 using a total predefined number "T" of sets.

1 6. The method of Claim 1, wherein the error-correcting code is associated with a compact
2 generating function and the method further comprises storing the compact generating function and
3 an index of one and only one stored set of keys, whereby no set of keys other than the index of the
4 stored set of keys need be stored in that sets of keys can be regenerated using the compact generating
5 function and the index of the stored set.

1 7. The method of Claim 6, wherein the compact generating function is a generating
2 matrix G, and the method further comprises transforming the compact generating function G to have
3 a non-systematic row assignment.

1 8. The method of Claim 1, wherein the error-correcting code generates vectors over an
2 alphabet having symbols, and the method further comprises renaming at least one symbol based on
3 a pseudorandom permutation.

1 9. A computer program device, comprising:

2 a computer program storage device including a program of instructions usable by a
3 computer, comprising:

4 logic means for defining, based on at least one error-correcting code, plural sets of
5 keys useful by respective devices for decrypting encrypted content.

1 10. The device of Claim 9, wherein each set represents a set of coordinates in a key
2 matrix.

1 11. The device of Claim 9, further comprising logic means for associating plural sets of
2 keys with respective devices.

1 12. The device of Claim 9, wherein the error-correcting code is a Reed-Solomon code.

1 13. The device of Claim 9, wherein the means for defining includes:
2 logic means for receiving at least a row parameter "N" representing the number of
3 rows in the key matrix and a column parameter "n" representing the number of columns in
4 the key matrix;

5 logic means for using an error-correcting code having a Hamming distance "d" that
6 minimizes key overlap between sets of keys.

1 14. The device of Claim 13, wherein the error-correcting code defines the sets of keys
2 using a total predefined number "T" of sets.

1 15. The device of Claim 9, wherein the error-correcting code is associated with a compact
2 generating function, and the device further comprises logic means for storing the compact generating
3 function and an index of a stored set of keys, whereby no sets of keys need be stored in that sets of
4 keys can be regenerated using the compact generating function and the index of the stored set.

1 16. The device of Claim 15, wherein the compact generating function is a generating
2 matrix G, and the device further comprises logic means for transforming the generating matrix G to
3 have a non-systematic row assignment.

1 17. The device of Claim 9, wherein the error-correcting code generates vectors over an
2 alphabet having symbols, and the device further comprises logic means for renaming at least one
3 symbol based on a pseudorandom permutation.

1 18. A computer programmed with instructions to cause the computer to execute method
2 acts including:

3 receiving, as input, at least a number "n" representing a number of columns in a key
4 matrix and a number "N" representing a number of rows in the key matrix, each position in
5 the key matrix being definable by a respective index, each index being associated with a
6 respective key useful by a decryption device for decrypting encrypted content;

7 defining, based at least in part on the input, plural sets of keys using a non-random
8 function.

9 19. The computer of Claim 18, wherein the non-random function is an error-correcting
10 code.

1 20. The computer of Claim 19, wherein the error-correcting code is a Reed-Solomon code.

1 21. The computer of Claim 18, wherein the method executed by the computer further
2 includes assigning at least some sets of keys to at least some respective devices.

1 22. The computer of Claim 19, wherein the error-correcting code is associated with a
2 generating matrix G, and the method executed by the computer further comprises storing the
3 generating matrix G and an index of a stored set of keys, whereby no set of keys other than the index
4 of the stored set of keys need be stored in that sets of keys can be regenerated using the generating
5 matrix G and the index of the stored set.

23. The computer of Claim 22, wherein the method executed by the computer further
comprises transforming the generating matrix G to have a non-systematic row assignment.

24. The computer of Claim 18, wherein the error-correcting code generates vectors over
an alphabet having symbols, and the method executed by the computer includes renaming at least one
symbol based on a pseudorandom permutation.

1 25. The method of Claim 4, wherein the error-correcting code is a linear code.

1 26. The device of Claim 9, wherein the error-correcting code is a linear code.

1 27. The computer of Claim 19, wherein the error-correcting code is a linear code.